

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION**

THE PACID GROUP, LLC

Plaintiff,

v.

APPLE, INC., et al.,

Defendants.

Civil Action No. 6:09-cv-143-LED-JDL

**PLAINTIFF THE PACID GROUP, LLC'S REPLY BRIEF
REGARDING CLAIM CONSTRUCTION**

TABLE OF CONTENTS

	Page No.
I. INTRODUCTION.....	1
II. THE LAW DOES NOT REQUIRE THE COURT TO PROVIDE AN EXPRESS CONSTRUCTION FOR ALL TERMS WHERE IT CONCLUDES THE ORDINARY MEANING IS APPROPRIATE.	1
III. DISPUTED CLAIM TERMS.....	2
A. “Pseudo-Random”	2
B. “Secure Hash Operation,” “Secure Hash Computer Program,” and “Secure Hash Algorithm”.....	4
C. Performing A Secure Hash Operation On Said Shuffled Bit Result To Produce A Message Digest: No Separate Construction Required	6
D. Shuffled Bit Result	6
E. Host System	7
F. Information File.....	8
G. Concatenating	9
H. Algebraic Function	9
I. Constant Value	10
J. Interrupt Control Means: Hardware Or Software That Issues A Signal To Interrupt The Operation Of A Processor.	10
IV. CONCLUSION	11

TABLE OF AUTHORITIES

Page No

Cases

<i>Alcatel USA Sourcing, Inc. v. Microsoft Corp.</i> , Case No. 6:06 CV 499, 2008 U.S. Dist. LEXIS 64351 (E.D. Tex. Aug. 21, 2008)	2
<i>Altiris, Inc. v. Symantec Corp.</i> , 318 F.3d 1363 (Fed. Cir. 2003).....	5
<i>E-Pass Techs., Inc. v. 3COM Corp.</i> , 343 F.3d 1364 (Fed. Cir. 2003).....	2, 9
<i>Home Diagnostics, Inc. v. LifeScan, Inc.</i> , 381 F.3d 1352 (Fed. Cir. 2004).....	8
<i>Medimmune, LLC v. PDL Biopharma, Inc.</i> , Case No. C 08-05590, 2010 U.S. Dist. LEXIS 21169 (N.D. Cal. Feb. 22, 2010).....	2-3
<i>Network-I Sec. Solutions, Inc. v. Cisco Sys.</i> , No. 6:08CV30, 2010 U.S. Dist. LEXIS 12938 (E.D. Tex. Feb. 16, 2010)	1
<i>O2 Micro Int’l Ltd. v. Beyond Innovation Tech. Co.</i> , 521 F.3d 1351 (Fed. Cir. 2008).....	1
<i>ReedHycalog UK, Ltd. v. Baker Hughes Oilfield Operations Inc.</i> , No. 6:06-cv-222, 2008 U.S. Dist. LEXIS 40877 (E.D. Tex. May 21, 2008)	1
<i>Saffran v. Boston Sci. Corp.</i> , 2008 U.S. Dist. LEXIS 52557 (E.D. Tex. July 9, 2008)	8

I. INTRODUCTION

Defendants’ proposed constructions should be rejected because they ignore fundamental principles of claim construction and are geared at forwarding their non-infringement or invalidity arguments rather than assisting the jury’s understanding of the patents in suit. For example, for some terms, they would import unwarranted limitations into the claims; in others, they would apply a construction separated from the context of the intrinsic record. Defendants’ constructions are apparently attempts to further some non-infringement or invalidity arguments, and they are inappropriate, incorrect, and contrary to the law.

PACid’s proposed constructions properly rely on intrinsic evidence and are consistent with the extrinsic evidence. Accordingly, PACid’s proposed constructions should be adopted.

II. THE LAW DOES NOT REQUIRE THE COURT TO PROVIDE AN EXPRESS CONSTRUCTION FOR ALL TERMS WHERE IT CONCLUDES THE ORDINARY MEANING IS APPROPRIATE.

Defendants argue in their opposition Defendants’ Claim Construction Brief (“Opp.”) that several claim terms must be expressly construed because Defendants have put the scope of the elements at issue by proposing particular constructions while PACid contends that they require no construction and their ordinary meanings apply. (Opp. at 12, 15-16, 18, 22, 23, 26.) Defendants argue that their position is supported by *O2 Micro Int’l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351 (Fed. Cir. 2008), but this Court has repeatedly rejected this argument. A decision in favor of PACid (*i.e.*, no construction is needed because the ordinary meaning applies) will resolve the dispute as to the claim scope, thereby satisfying the requirements of *O2 Micro*. See, *e.g.*, *Network-1 Sec. Solutions, Inc. v. Cisco Sys.*, No. 6:08CV30, 2010 U.S. Dist. LEXIS 12938, at *40 (E.D. Tex. Feb. 16, 2010) (rejecting defendants attempt to rewrite claims to reflect the disclosed embodiment and finding that no construction “resolved the parties’ dispute” pursuant to *O2 Micro*) (Ex. E)¹; *ReedHycalog UK, Ltd. v. Baker Hughes Oilfield*

¹ Exhibits E-J hereto are attached to the Declaration of Stanley H. Thompson, Jr. in Support of Plaintiff The PACid Group, LLC’s Reply Brief Regarding Claim Construction, filed concurrently herewith. Exhibits A and B hereto were attached to the Declaration of Stanley H. Thompson, Jr. in Support of Plaintiff The PACid Group, LLC’s Opening Brief Regarding Claim

Operations Inc., No. 6:06-cv-222, 2008 U.S. Dist. LEXIS 40877, at *5 (E.D. Tex. May 21, 2008) (“a court may decline to construe a claim term or rely on that term’s ordinary meaning if the court resolves the parties’ claim-scope dispute and precludes the parties from presenting jury arguments inconsistent with the court’s adjudication of claim scope”) (Ex. F); *Alcatel USA Sourcing, Inc. v. Microsoft Corp.*, Case No. 6:06 CV 499, 2008 U.S. Dist. LEXIS 64351, at *19-22 (E.D. Tex. Aug. 21, 2008) (“The claims provide the context such that construction of the ‘comparing’ step is not necessary.”). (Ex. G.)

Defendants’ argument that the Court cannot conclude that the ordinary meaning applies to some claim terms and that no further construction is necessary for those terms is incorrect and should be rejected.

III. DISPUTED CLAIM TERMS

A. “Pseudo-Random”

<u>PACID’S CONSTRUCTION</u>	<u>DEFENDANTS’ CONSTRUCTION</u>
No construction necessary. If construed: apparently random, but repeatable and predictable.	Refers to output that is repeatable and predictable to anyone who knows the function’s inputs but appears to be totally random to those without such knowledge.

Defendants attempt to justify their unduly narrow construction of “pseudo-random” by arguing that the ’646 Patent and the ’612 Patent contain a “definition” of this term. (Opp. at 3-4.) The ’646 Patent and the ’612 Patent do not define “pseudo-random” but, in describing the preferred embodiments, do provide substantial context for the construction, upon which PACid’s alternative construction is based. “[I]n determining whether a statement by a patentee was intended to be lexicographic, it is important to determine whether the statement was designed to define the claim term or to describe a preferred embodiment.” *E-Pass Techs., Inc. v. 3COM Corp.*, 343 F.3d 1364, 1369 (Fed. Cir. 2003) (finding that a description of the earlier technology and of a preferred embodiment is not a lexicographic definition). Even if a patent uses phrases such as “as used herein” these are not necessarily definitional. *See Medimmune, LLC v. PDL*

Construction, previously filed.

Biopharma, Inc., Case No. C 08-05590, 2010 U.S. Dist. LEXIS 21169, at *14-17 (N.D. Cal. Feb. 22, 2010) (concluding that “as used herein, the term ‘humanized’ immunoglobulin refers to” did not signify a definition of “humanized immunoglobulin”) (citing *E-Pass Techs., Inc.*). (Ex. H.)

Both the ’646 Patent and the ’612 Patent state the following: “The term ‘pseudo-random’ as used in this specification means that the output referred to is repeatable and predictable to anyone who knows the E-Key seed input to the function producing the output. Without such knowledge, the output appears to be totally random.” (Ex. A, Col. 5, ll. 14-18; Ex. B, Col. 4, ll. 1-4.) This appears in the section labeled “DESCRIPTION OF PREFERRED EMBODIMENTS” in each patent and is not a definition.

PACid relies appropriately on this portion of the specifications. As stated in the Opening Brief, this portion of specification includes the essential properties of a pseudo-random output, *i.e.*, that it is repeatable and predictable, yet apparently random. These properties are included in PACid’s proposed construction. Defendants’ own expert, Dr. Mercer agrees:

Q. Do you know what pseudorandom means?

....

A. Pseudorandom means that usually there is a binary string of digits that may be a single string or it may be a parallel string, and the objective is to have that set of digits exhibit properties that would be associated with mutual statistical independence. But on the other hand, that word “pseudo” is there because the underlying basis by which that string is generated is not, in fact, truly random. *It’s a deterministic approach to producing what seems to be random.*

(Ex. I, Transcript of the Deposition of M. Ray Mercer, Ph.D. (rough) at 28:4-15 (emphasis added).)

Defendants’ proposed construction improperly includes limitations from the preferred embodiments and results in language that cannot easily be substituted into the surrounding claim. Accordingly, PACid respectfully requests that the Court adopt its proposed construction of “pseudo-random”: “apparently random, but repeatable and predictable.”

B. “Secure Hash Operation,” “Secure Hash Computer Program,” and “Secure Hash Algorithm”

<u>PACID’S CONSTRUCTION</u>	<u>DEFENDANTS’ CONSTRUCTION</u>
Secure Hash Operation: An algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output.	Secure Hash Operation: An operation that can accept an input of variable bit length, but always produces an output having the same bit length such that it is computationally infeasible to determine (a) the input from the output and (b) two inputs that produce the same output, and where if a single bit of the input is changed, on average approximately 50% of the output bits are changed
Secure Hash Computer Program: No separate construction necessary due to the construction of “secure hash operation.” If construed: a computer program that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output.	Secure Hash Computer Program: computer program that uses a secure hash algorithm
Secure Hash Algorithm: No separate construction necessary due to the construction of “secure hash operation.” If construed: an algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output.	Secure Hash Algorithm: An algorithm that can accept an input of variable bit length, but always produces an output having the same bit length such that it is computationally infeasible to determine (a) the input from the output and (b) two inputs that produce the same output, and where if a single bit of the input is changed, on average approximately 50% of the output bits are changed.

Defendants argue that the construction of “secure hash” should include several separate limiting concepts. (Opp. at 5-11.) PACid agrees that two of these concepts ((1) that the output is deterministic, e.g., no two inputs produce the same output, and (2) that the output has no known relationship with the input that may be used to recover the input from the output) are appropriate. However, the Defendants’ inclusion of the additional limitations improperly import limitations from the embodiments in the specification into the claims.

First, Defendants would require that a secure hash operation “always produces an output having the same bit length.” (Opp. at 6-7.) This, however, would read out an expressly disclosed preferred embodiment. The specification describes hash algorithms and provides

several examples: “The hash function itself may be any of the well-known hash functions including those set forth in Table I below.” (Ex. A, ’646 Patent, 5:25-27.) Table I includes the “HAVAL” hash function and indicates that the output hash length is “Variable.” *Id.*, 5:37. Defendants’ resorting to extrinsic evidence to contradict the intrinsic evidence is to no avail. *Altiris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1369 (Fed. Cir. 2003) (“Extrinsic evidence may never be relied upon, however, to vary or contradict the clear meaning of terms in the claims.”). Defendants’ construction is simply incorrect.

Second, Defendants are improperly seeking to incorporate the term “computationally infeasible” in their proposed construction. (Opp. at 8-10.) Defendants admit that the inventors themselves did not use the term “computationally infeasible.” Rather this term comes from a reference cited in the specification of the ’612 Patent. Even if this reference were considered intrinsic evidence, the inventors stated that it provides “[g]eneral background” and it appears in the section labeled “BACKGROUND OF THE INVENTION.” Defendants concede that the words used in the specifications of the patents-in-suit are “[t]here is no known relationship between the input and output of a hash algorithm which may be used to recover the input from the output.” (Opp. at 8; Ex. A, Col. 2, ll. 8-10; Ex. B, Col. 2, ll. 15-17.) PACid’s proposed construction uses the same words. Defendants’ introduction of “computationally infeasible” improperly imports an unclaimed limitation into their proposed construction and will be confusing to a jury.

Third, Defendants’ proposed construction requiring that “if a single bit of the input is changed, on average approximately 50% of the output bits are changed” improperly attempts to import a limitation from the specification. (Opp. at 10-11.) Furthermore, the language of Defendants’ construction—“on average approximately 50%”—is unclear and complicates the construction unnecessarily. Moreover, Defendants argue, without supporting citation, that an algorithm with a deterministic output that has a constant length and that has no known relationship with the input that may be used to recover the input from the output “will satisfy

strict avalanche criteria.” To the extent this is true, it indicates that adding this limitation is unnecessary.

Accordingly, the Court should adopt PACid’s proposed construction, which includes the key properties of secure hash operations that (1) the output is deterministic, e.g., no two inputs produce the same output, and (2) that the output has no known relationship with the input that may be used to recover the input from the output, and reject Defendants’ construction, which includes additional inappropriate and unnecessary limitations.

C. Performing A Secure Hash Operation On Said Shuffled Bit Result To Produce A Message Digest: No Separate Construction Required

<u>PACID’S CONSTRUCTION</u>	<u>DEFENDANTS’ CONSTRUCTION</u>
No separate construction necessary.	The input to the secure hash operation is the shuffled bit result from step (a), and the output of the secure hash operation is a message digest.

The Defendants fail to address the central issue regarding the construction of this phrase. (Opp. at 11-15.) If the words in the phrase collectively do not connote a different meaning than the plain or construed meanings of its individual terms, the phrase as a whole does not need to be construed. For example, the term “baseball diamond” would need a separate construction from “baseball” and “diamond” because “baseball diamond” connotes something different from the two terms that comprise it. Defendants do not argue in their opposition that this is the case for the phrase at issue. Therefore, PACid proposes that no separate construction is necessary for the phrase “performing a secure hash operation on said shuffled bit result to produce a message digest” as the jury should apply its plain meaning in light of the construction of “secure hash operation” and “shuffled bit result.”

D. Shuffled Bit Result

<u>PACID’S CONSTRUCTION</u>	<u>DEFENDANTS’ CONSTRUCTION</u>
The result of an operation that mixes the bits of its inputs.	The result of an operation that randomly mixes and maps the bits of its inputs.

Defendants’ construction of shuffled bit result requires the additional limitations that it “randomly” mixes “and maps” the bits of its inputs. (Opp. at 15-16.) First, the additional requirement of “randomly” should be rejected because it erroneously (or at least unclearly)

requires a random process when the specification is clear that the result is a pseudo-random number. (Ex. A, '646 Patent, 3:22-28 (“a bit-shuffling which results in the mapping of a large number of bits into a first pseudo-random number”); Ex. B, '612 Patent, 3:18-24 (“shuffles the bits and provides a pseudo-random result”).) Second, Defendants’ primary support for the “mixes and maps” does not support the double requirement. Instead, the summary of the invention refers only to a single requirement of bit shuffling, with the single example of mapping bits. While other portions of the specification use the words “mixed” and “mapped,” these are similar terms describing the same bit shuffling process. Because the term “shuffled” in this context means “mixed” and this meaning is readily understood by a lay jury (and more so than the less accessible term “mapped”), the Court should adopt PACid’s proposed construction.

E. Host System

<u>PACID’S CONSTRUCTION</u>	<u>DEFENDANTS’ CONSTRUCTION</u>
No construction necessary. If construed: a system for providing command sequences.	Computer that inputs command sequences to an encryption key generator.

Defendants’ complaint that PACid’s construction does not identify the recipient of the command sequence is not well taken. (Opp. at 18-19.) Claim 12 identifies what receives the command sequence—the claimed I/O interface. (Ex. A, 9:52-54.) Thus, it is both unnecessary and improper to incorporate this information into the construction of “host system.”

Defendants’ construction limiting the host system to a computer is an apparent attempt to fabricate a non-infringement position that the host system is computer separate from the remainder of the system and is simply improper. “Absent a *clear disavowal* or contrary definition in the specification or the prosecution history, the patentee is entitled to the full scope of its claim language.” *Home Diagnostics, Inc. v. LifeScan, Inc.*, 381 F.3d 1352, 1358 (Fed. Cir. 2004) (emphasis added). In the context of the claims, the host system is a provider of command sequences, nothing more. Defendants attempt to import limitations from the definition of “host” from extrinsic evidence is improper. A court should not incorporate dictionary definitions with “no basis in the specification or record for selecting one of the definitions.” *Saffran v. Boston*

Sci. Corp., 2008 U.S. Dist. LEXIS 52557, at *2-3 (E.D. Tex. July 9, 2008). (Ex. J.) Indeed, a portion of a preferred embodiment in the specification is a Motorola integrated circuit MC68HC05SC28, which is simply a chip that can be combined with the host system. (Ex. A, '646 Patent, 7:22-28.) Defendants' proposed inclusion of the word "computer" in the construction of host system is unclear and, to the extent it suggests a separate enclosure, display, keyboard, mouse, etc., it is inconsistent with the context of the specification.

The Court should apply the ordinary meaning of this term, or alternatively, if the Court concludes that the term must be construed, it should adopt PACid's proposed construction.

F. Information File

<u>PACID'S CONSTRUCTION</u>	<u>DEFENDANTS' CONSTRUCTION</u>
Message or file.	A collection of information stored as a unit and identified by a unique name.

Defendants misrepresent the prosecution history by implying that the patentees were disclaiming "message" when they amended Claim 1 to recite "information file." (Opp. at 20-21.) An examination the text of the claim as it was written before that amendment reveals that the motivation for the change from "message" to "information file" was to give the term an antecedent basis because the term "message" was not previously used in the claim, whereas "information file" appears in the preamble. (Opp., Ex. 10 (12/28/98 Amendment) at 1-2 (4-5 of D.I. 265-11).) The implication of this amendment is actually the opposite of what Defendants argue. This full context reveals that the patentees intended to include "message" but discovered a drafting error in that it lacked an antecedent basis, so they amended it with a term that was broader and that had an antecedent basis.

In addition, Defendants' construction is fatally flawed in that it requires information "stored as a unit" and "identified by a unique name." Neither of these two additional limitations is supported by intrinsic evidence. As Defendants' admission that the information "does not need to be contiguously stored in memory" suggests (Opp. at 21), the additional language "stored as a unit" implies otherwise and could be confusing to a jury. Also, Defendants provide no

support for its requirement that an information file be “identified by a unique name.” Defendants’ construction must be rejected.

PACid’s proposed construction is fully supported by the specification’s description of an “information file” more specifically as a “message or file”: “The invention relates generally to a method and system for *protecting an information file* from unauthorized access, and *more specifically to the encryption of a message or file*” (Ex. B, ’612 Patent, 1:8-10.) Accordingly, PACid’s proposed construction should be adopted.

G. Concatenating

<u>PACID’S CONSTRUCTION</u>	<u>DEFENDANTS’ CONSTRUCTION</u>
No construction necessary. If construed: linking units together.	Placing one bit field directly next to another.

As discussed above, it is inappropriate to convert a description of a preferred embodiment into a so-called definition. *See E-Pass Techs.*, 343 F.3d at 1369. In any event, Defendants’ argument requires extrinsic evidence in the form of a dictionary definition of “juxtapose,” which does not support the Defendants’ additional limitation requiring that one bit field be placed “directly” next to another. Accordingly, the Defendants’ construction should be rejected, and the Court should conclude that the ordinary meaning applies or alternatively if express construction is required, should adopt PACid’s proposed construction.

H. Algebraic Function

<u>PACID’S CONSTRUCTION</u>	<u>DEFENDANTS’ CONSTRUCTION</u>
No construction necessary. If construed: any operation used in mathematics.	Any operation used in mathematics or logic.

Defendants argue for their proposed construction by attempting to use the structure of Claim 1 and its dependent Claim 4 of the ’612 Patent. (Opp. at 23-24.) Claim 1 recites a combining step that includes an algebraic function. Claim 4 recites that the combining step of Claim 1 also includes one or more logic functions, not that the algebraic function of Claim 1 must include one or more logic functions, which is the implication of Defendants’ argument. The fact that dependant claims separately claim algebraic, logic, and cryptographic functions

(e.g., Ex. B, '612 patent, Claims 3-5) supports PACid's construction that an algebraic function is separate from a logic function. Accordingly, the Court should adopt PACid's understanding of this term.

I. Constant Value

<u>PACID'S CONSTRUCTION</u>	<u>DEFENDANTS' CONSTRUCTION</u>
No construction necessary. If construed: A value that does not change for any given instance of generating an encryption key.	A value that does not change.

Defendants' argument regarding "constant value" borders on sophistry. (Opp. at 26-27.) There is no basis whatsoever in the specification for construing "constant value" as a reference to values like pi, the base of the natural logarithm, *e*, the gravitational constant, or any other value from mathematics or nature. In its Opening Brief, PACid provided intrinsic evidence from the specification that describes examples of a constant value as having several different components that can be *changed*. For example, a constant value can include an E-Key Seed ID, and the user may choose to assign *another* E-Key Seed ID. (Ex. B, '612 patent, 6:13-18 ("When the constant value 11 is first being formed, the E-Key Seed ID is automatically entered as that of the host system. A user is prompted, however, to either accept the ID or assign another. In this manner, files may be shared between PCs, workstations, and workgroups that normally use different E-Key Seeds.").) The patent is describing a constant in the context of an encryption/decryption process, not the context of mathematic or natural laws, and Defendants' deliberate attempt at obfuscation is not well taken. Accordingly, PACid's understanding of this term should be adopted.

J. Interrupt Control Means: Hardware Or Software That Issues A Signal To Interrupt The Operation Of A Processor.

PACid incorporates by reference herein its opposition to Defendants' motion for summary judgment that claims 12 and 26 are indefinite.

IV. CONCLUSION

For all of the foregoing reasons, the Court should adopt PACid's proposed understandings of the disputed claim terms.

Dated: March 15, 2010

Respectfully submitted,

By: /s/ Stanley H. Thompson, Jr.
Marc A. Fenster, CA Bar # 181067
Email: mfenster@raklaw.com
Stanley H. Thompson, Jr., CA Bar # 198825
Email: sthompson@raklaw.com
Alexander C. Giza, CA Bar # 212327
Email: agiza@raklaw.com
Andrew D. Weiss, CA Bar # 232974
Email: aweiss@raklaw.com
RUSS, AUGUST & KABAT
12424 Wilshire Blvd., 12th Floor
Los Angeles, California 90025
Telephone: 310/826-7474
Facsimile: 310/826-6991

Andrew W. Spangler, TX Bar # 24041960
Email: spangler@spanglerlawpc.com
LEAD COUNSEL
SPANGLER LAW P.C.
208 N. Green Street, Suite 300
Longview, Texas 75601
Telephone: 903/753-9300
Facsimile: 903/553-0403

Elizabeth A. Wiley, TX Bar # 00788666
THE WILEY FIRM, PC
Email: lizwiley@wileyfirmnpc.com
P.O. Box. 303280
Austin, Texas 78703-3280
Telephone: 512/420-2387
Facsimile: 512/551-0028

Robert P. Kelly, MI SB # P72574
E-mail: Robert@robertpkellypllc.com
ROBERT P. KELLY PLLC
938 Chester
Birmingham, MI 48009
Telephone: 248/703-8760
Facsimile: 248/251-0267

Attorneys for Plaintiff
PACID, LLC

CERTIFICATE OF SERVICE

I hereby certify that the following counsel of record who are deemed to have consented to electronic service are being served on March 15, 2010, with a copy of this document via the Court's CM/ECF system. Any other counsel of record will be served by first class U.S. mail on this same date.

By: /s/ Stanley H. Thompson, Jr.
Stanley H. Thompson, Jr.